THE
AMERICAN
MATHEMATICAL MONTHLY.

Entered at the Post-office at Springfield, Missouri, as second-class matter.

VOL XVIII. MARCH, 1911. NO. 3.

TESTS OF SYMMETRIC POLYNOMIALS.

By DR. G. A. MILLER, University of Illinois.

In Bôcher's *Introduction to Higher Algebra*, 1907, page 240, the following theorem is stated: *A necessary and sufficient condition for a polynomial to be symmetric is that it be unchanged by every interchange of two variables.* This test becomes quite laborious even when the number of variables is reasonably small; for instance, for six variables there are fifteen distinct pairs of variables so that this theorem requires fifteen trials to prove that a polynomial in six variables is symmetric. In general, the number of trials according to the given theorem is clearly $\frac{n(n-1)}{2}$, and hence this number increases very rapidly with n. In view of this fact, it may be of interest to consider some tests requiring a very much smaller number of trials, especially since the determination of these tests is equivalent to a determination of sets of generating substitutions of the symmetric group of degree n and hence it is a problem which is common to at least two subjects.

If the following well known theorem: *A necessary and sufficient condition for a polynomial to be symmetric is that it be unchanged by every interchange of two variables such that one variable is the same in each of these pairs of variables*, were substituted for the one given above, the number of trials necessary to prove the symmetry of a polynomial of n variables would evidently be reduced to $n-1$, and the individual trials would not involve any more labor than those of the theorem of the first paragraph. Moreover, the proof of the theorem of the present paragraph involves very little more thought than that of the preceeding paragraph. In fact the $\frac{n(n-1)}{2}$ possible transpositions, or interchanges of pairs of variables formed from n variables, can clearly be obtained by transforming the $n-1$, which have a common variable by means of others of this set of $n-1$ transpositions. That every possible transposition on these n variables may be obtained in this manner, results from the following identity:

$$a_\alpha a_\beta = a_1 a_\alpha \,.\, a_1 a_\beta \,.\, a_1 a_\alpha$$

If the polynomial is transformed into itself by a set of substitutions it must be invariant under the group generated by this set. As a symmetric polynomial is transformed into itself by all the possible substitutions on its variables, it results that we must always employ a set of generating substitutions of the symmetric group in proving that a polynomial is symmetric, as was remarked above. It is well known that every symmetric group is generated by two of its substitutions, and hence we do not need to employ more than two substitutions to prove or to disprove the symmetry of any polynomial. Moreover, since every symmetric group whose degree exceeds two is non-cyclic, we must always use at least two substitutions, when the number of variables exceeds 2, to prove or to disprove this symmetry.

Two generating substitutions of the symmetric group of degree n can be selected in a number of ways which increases rapidly with n. One such pair consists of an arbitrary cyclic substitution on the n variables and an arbitrary transposition not contained in a cycle of less than n variables in a power of this substitution. This fact may be stated more definitely as follows: *A necessary and sufficient condition that a cyclic substitution of degree n and a transposition on two of these n letters generate the symmetric group of degree n is that this transposition is not contained in any of the cycles of order less than n generated by this substitution.* The truth of this theorem is almost self-evident. It may, however, be regarded as a result of combining the following two well known theorems: If a primitive substitution group involves a transposition it is symmetric; a regular group having exactly k different sub-groups, besides the identity and the entire group, has also exactly k different systems of imprimitivity.*

One of the most useful theorems with respect to two generating substitutions of the symmetric group of degree n may be stated as follows: *If two cycles having only one common letter involve n different letters and if at least one of these cycles involves an even number of letters they must generate the symmetric group of the degree n.* The proof of this theorem results almost immediately from the fact that the commutator of the two given cycles is a cyclic substitution of order 3 according to a theorem due to Bochert.† The conjugates under these cycles of this substitution of order 3 generate the alternating group of degree n, and this alternating group together with the cycle of even order generates the symmetric group of degree n. The special case when the cycle which involves an even number of letters is a transposition, leads to the following corollary: *A necessary and sufficient condition for a polynomial in n variables to be symmetric is that it be unchanged by the cyclic interchange of some $n-1$ of these variables as well as by the interchange of the remaining variable and some one of these $n-1$ variables.*

---

* Dyck, *Mathematische Annalen*, Vol. 22 (1883), p. 89.

† *Mathematische Annalen*, Vol. 33 (1889), p. 587.

It is a very simple matter to state numerous other criterions for the symmetry of polynomials of n variables. In Netto's *Theory of Substitutions*, 1892, page 90, it is stated that the probability that any two substitutions on n letters generate the symmetric group may be taken as about $\frac{3}{4}$. That is, if we interchange the n variables of a polynomial according to two substitutions, and if the polynomial remains unchanged, the probability that it is symmetric is about $\frac{3}{4}$. Although this implies that numerous tests for symmetry may readily be obtained, it is doubtful whether it is possible to find more useful general tests than those given in the preceding paragraphs. Among the most convenient additional tests is the following: *A necessary and sufficient condition for a polynomial in n variables to be symmetric is that it be unchanged by each of the $n-1$ interchanges which result when we interchange the first and the second variable, then the second and third, then the third and fourth, and finally the $(n-1)$th and the nth.*

Although the last theorem requires $n-1$ tests to prove the symmetry of a polynomial, each of these tests is so very simple that the total number of them involve about the same amount of labor as each of the sets of two tests given in the preceding theorems. In this connection it may be observed that the symmetric group of degree n can always be generated by a pair of substitutions of orders 2 and 3 respectively, except when n is one of the three numbers 5, 6, 8.* Hence we may prove the symmetry of a polynomial of any degree, besides these three, by means of two substitutions of orders 2 and 3 respectively. In practice this kind of general test is, however, less simple than some of those given above. On the other hand, the noted Italian mathematician, Alfredo Capelli, gave a test which is fairly convenient and can be easily stated as follows: *A necessary and sufficient condition for a polynomial to be symmetric is that it be unchanged by a cyclic interchange of all its variables as well as by the cyclic interchange of all but one of its variables, the variables having the same relative positions in the two cycles.*†

Deep interest in the symmetric functions was first aroused by the fact that the coefficients of the general equation of degree n, are symmetric functions of the roots. In 1770, Lagrange and others began the study of rational integral functions of n variables which are not necessarily symmetric, and observed that the number of different formal values assumed by such functions, when the variables are permuted in every possible way, is always a division of $n!$ Just as the permutations which do not affect the formal value of a symmetric polynomial, correspond to a substitution group, so there is also connected with each non-symmetric polynomial a substitution group which sheds light on its properties. In particular the number of different formal values of the polynomial, when its variables are permuted in every possible manner, is equal to the index of this substitution group, and the possibility of constructing polynomials with a given number of

---

* *Bulletin of the American Mathematical Society*, Vol. 7 (1901), p. 426.

† Capelli, *Giornale di Matematiche*, Vol. 35 (1897), p. 354.

formal values, is completely determined by the possible substitution groups on these variables. The above remarks apply directly to all rational functions of the n variables as well as to the more special functions which are commonly (but not universally) called polynomials.

ON THE COMBINATION OF INVOLUTIONS.*

By D. N. LEHMER, University of California.

1. Given two involutions of rays in the same plane with centers at A and B a quadratic reciprocal transformation may be set up in the plane as follows: To any point P make correspond the intersection P' of the two rays at A and B which correspond in the involutions to the rays PA and PB. The point-to-point transformation thus defined is clearly involutorial. Certain points appear as exceptional in that the correspondence is not unique, namely: all of the points on the line joining A and B go by the transformation into the same point C. Further, all of the points on AC go into the same point B, and all of the points on BC go into the point A, as is seen by making the construction according to the definition. It will be suspected that the point C is the center of an involution which might be used instead of A or B to define the same transformation. That this is the case appears as a corollary from the following fundamental theorem.

2. Theorem. *If the point P describes a straight line the corresponding point P' describes a conic through A, B, and C.*

The point row P projects to A and B in two perspective pencils. The corresponding rays in the involutions at A and B are therefore projective and generate a conic through A and B. Since the point row P meets the line AB in one point the corresponding point P' goes through C. From the construction it appears further that the point row of the first order P is projective to the point row of the second order P'. It follows therefore that the pencils PC and $P'C$ are projective and that they are in involution. The point C is thus in all respects coördinate with A and B.

If we assume the theorem that a conic meets a curve of degree m in $2m$ points we may prove easily the more general theorem.

3. Theorem. *A curve of degree n goes by the above transformation into a curve of degree $2n$.*

For let the curve C of degree n go into a curve C'. Cut across C' by a line g. Transform C' and g. C' goes back into C and g goes into a conic γ. The points common to C and the conic γ, $2n$ in number, correspond to the points common to C' and the arbitrary line g.

* Presented at the September meeting of the San Francisco Section of the American Mathematical Society, under slightly different title.